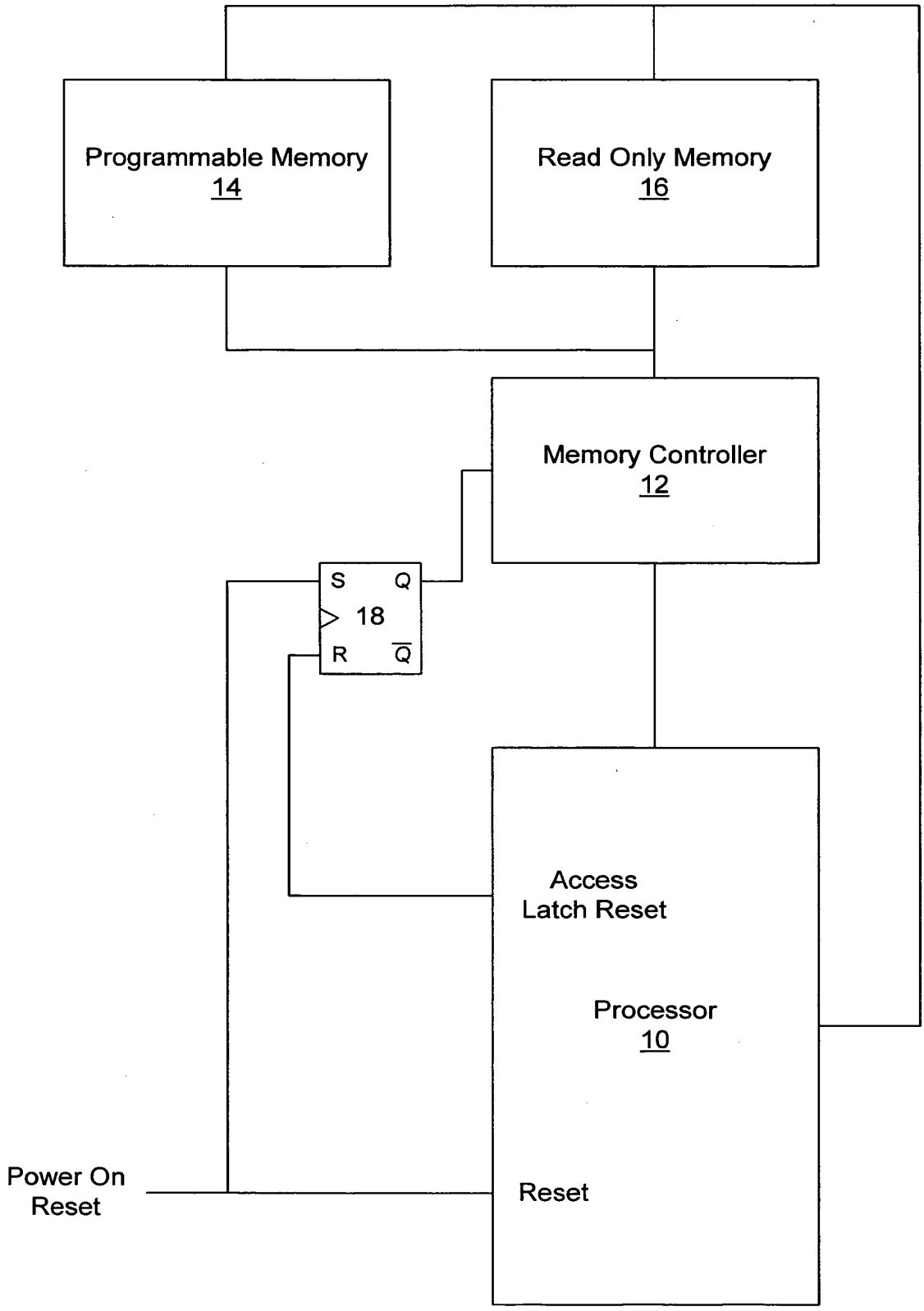

Programmable Memory
14
Read Only Memory
16
Memory Controller
12
S
Q
18
R
Q
Access
Latch Reset
Processor
10
Power On
Reset
Reset

Figure 1

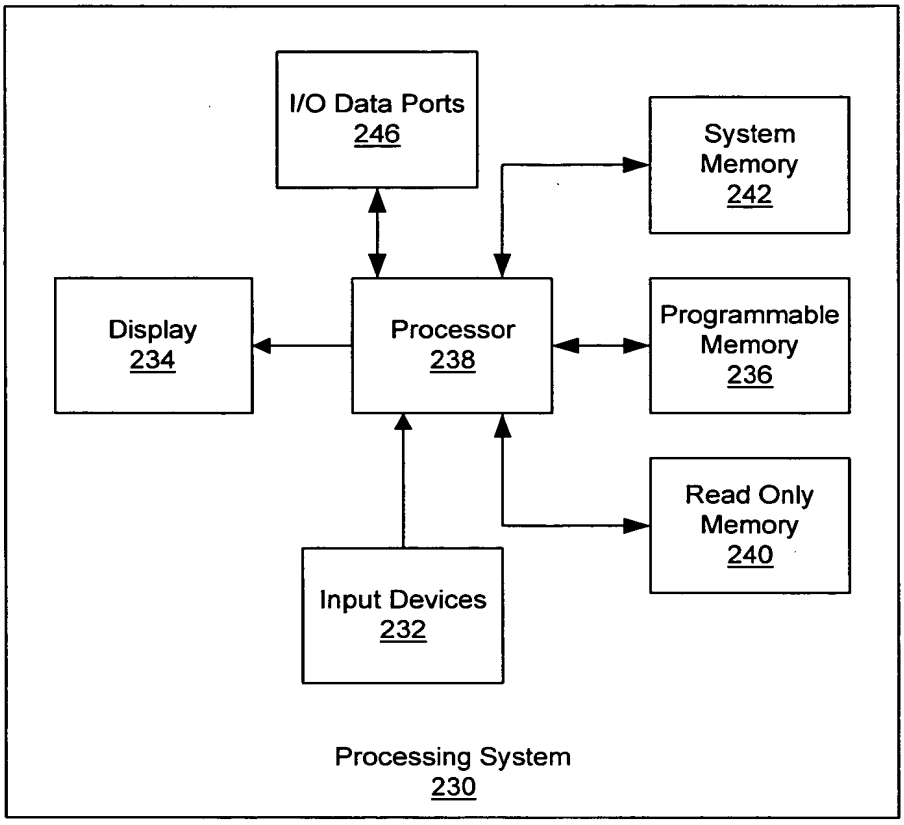

I/O Data Ports
246
System
Memory
242
Display
234
Processor
238
Programmable
Memory
236
Read Only
Memory
240
Input Devices
232
Processing System
230

Figure 2

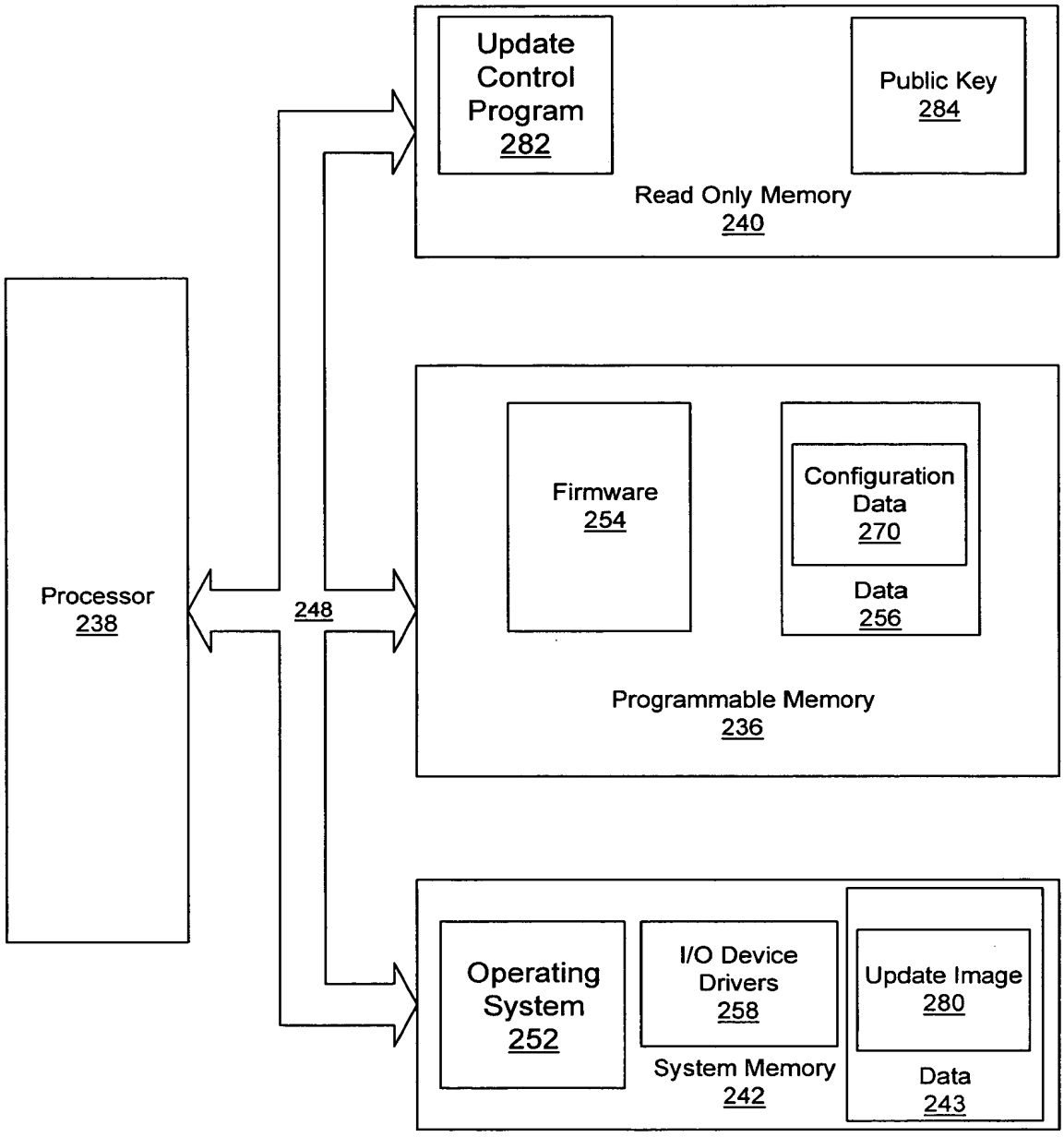

Update Control Program 282
Public Key 284
Read Only Memory 240
Processor 238
248
Firmware 254
Configuration Data 270
Data 256
Programmable Memory 236
Operating System 252
I/O Device Drivers 258
Update Image 280
System Memory 242
Data 243

Figure 3

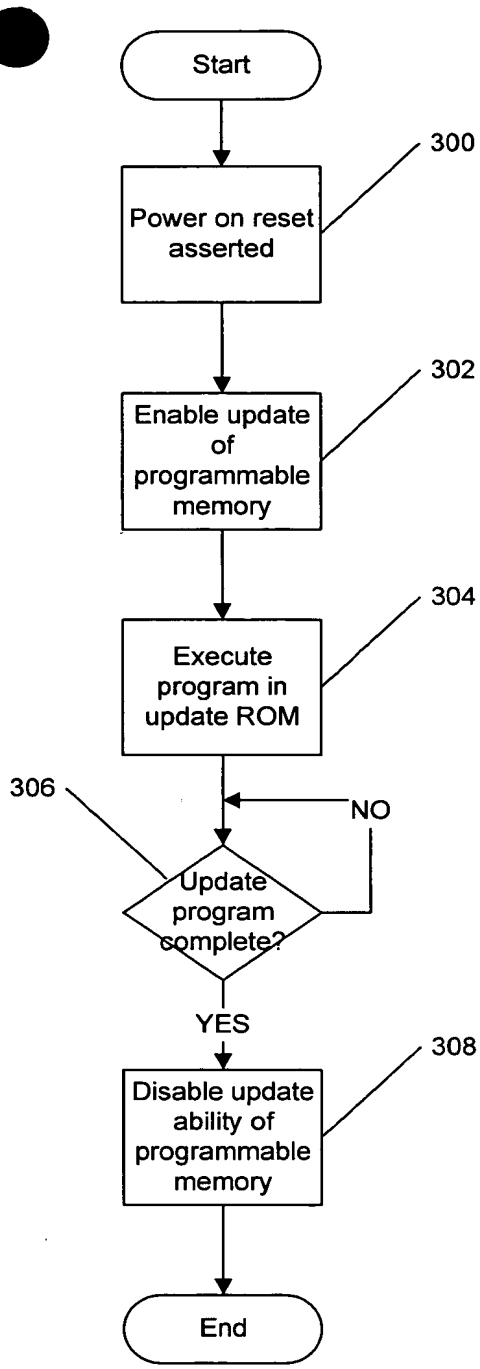

Start
300
Power on reset asserted
302
Enable update of programmable memory
304
Execute program in update ROM
306
NO
Update program complete?
YES
308
Disable update ability of programmable memory
End

Figure 4A

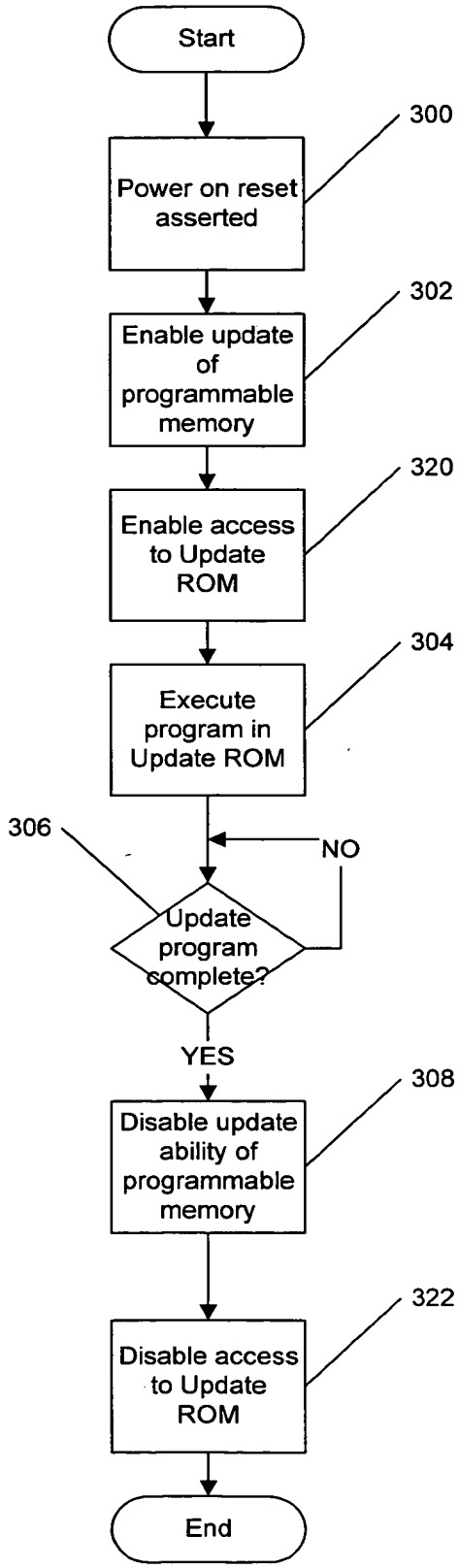
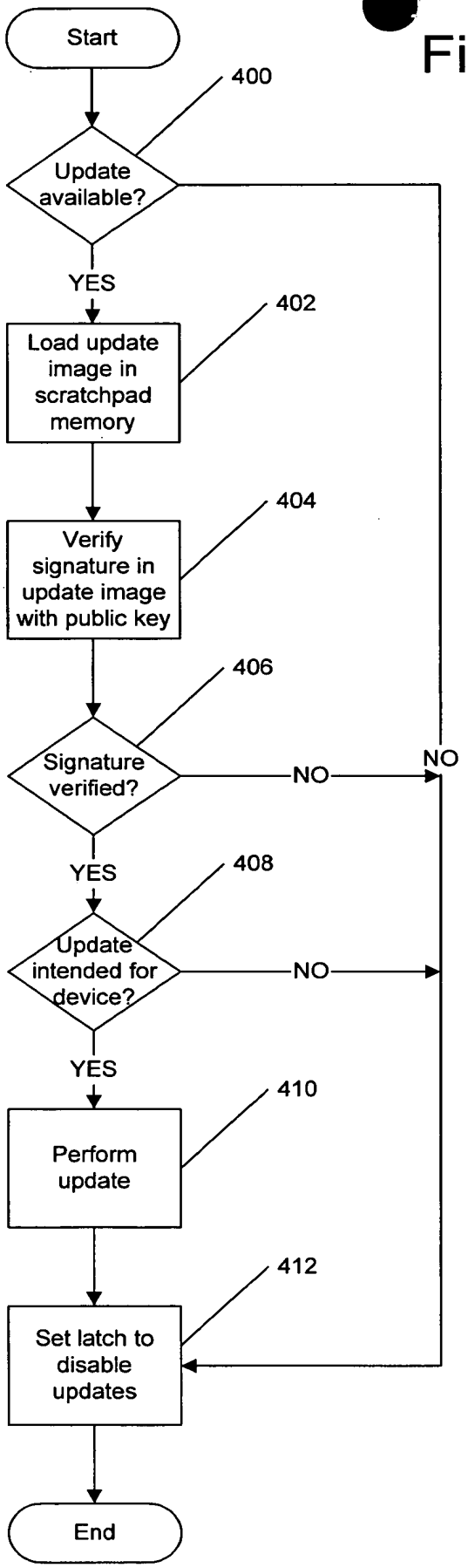

Start
300
Power on reset asserted
302
Enable update of programmable memory
320
Enable access to Update ROM
304
Execute program in Update ROM
306
NO
Update program complete?
YES
308
Disable update ability of programmable memory
322
Disable access to Update ROM
End

Figure 4B

Figure 5


Start
400
Update available?
YES
NO
402
Load update image in scratchpad memory
404
Verify signature in update image with public key
406
Signature verified?
NO
YES
408
Update intended for device?
NO
YES
410
Perform update
412
Set latch to disable updates
End

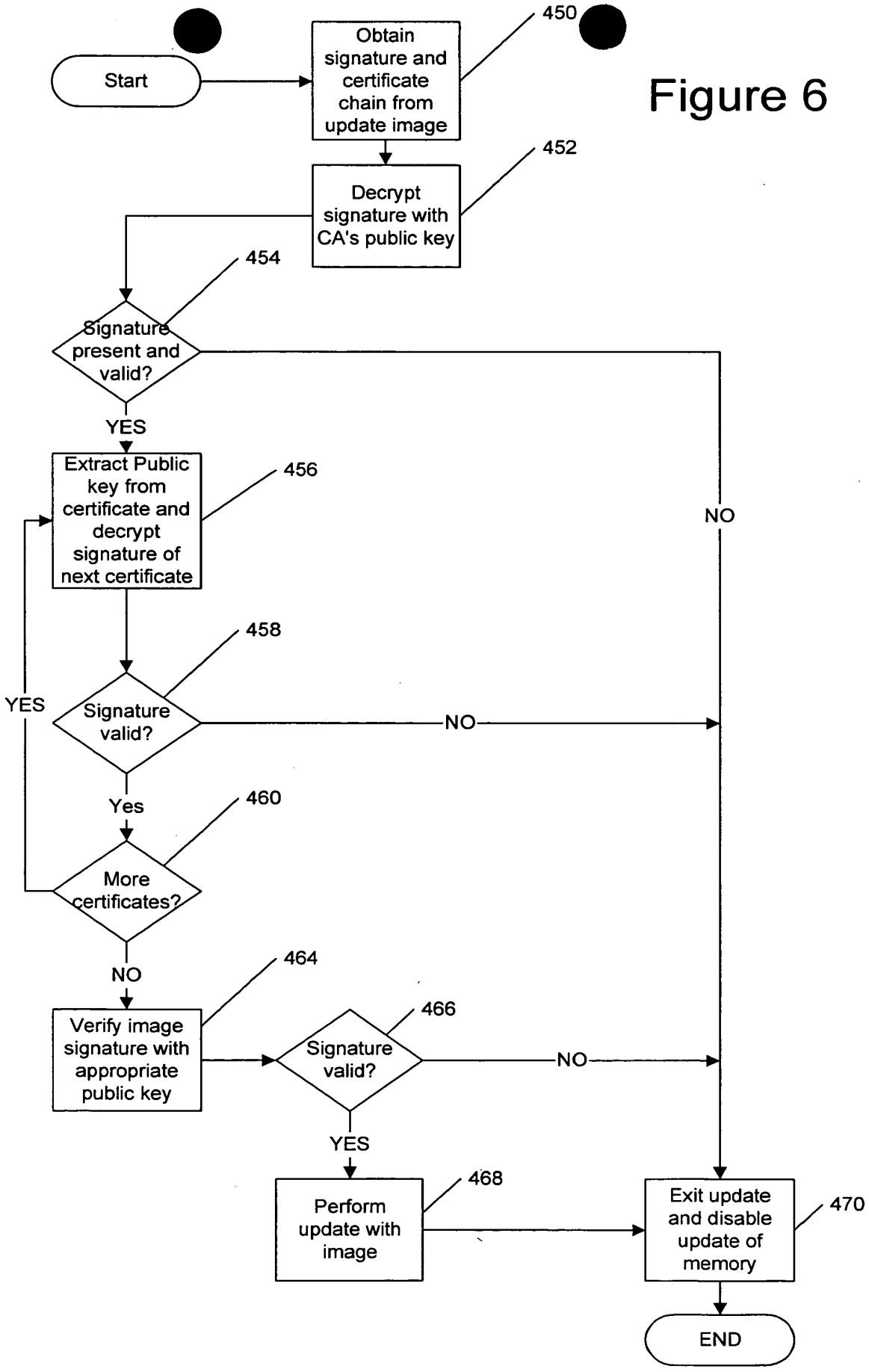

Start
Obtain signature and certificate chain from update image
450
Decrypt signature with CA's public key
452
454
Signature present and valid?
YES
NO
Extract Public key from certificate and decrypt signature of next certificate
456
458
Signature valid?
YES
NO
Yes
460
More certificates?
NO
464
Verify image signature with appropriate public key
466
Signature valid?
NO
YES
468
Perform update with image
Exit update and disable update of memory
470
END

Figure 6

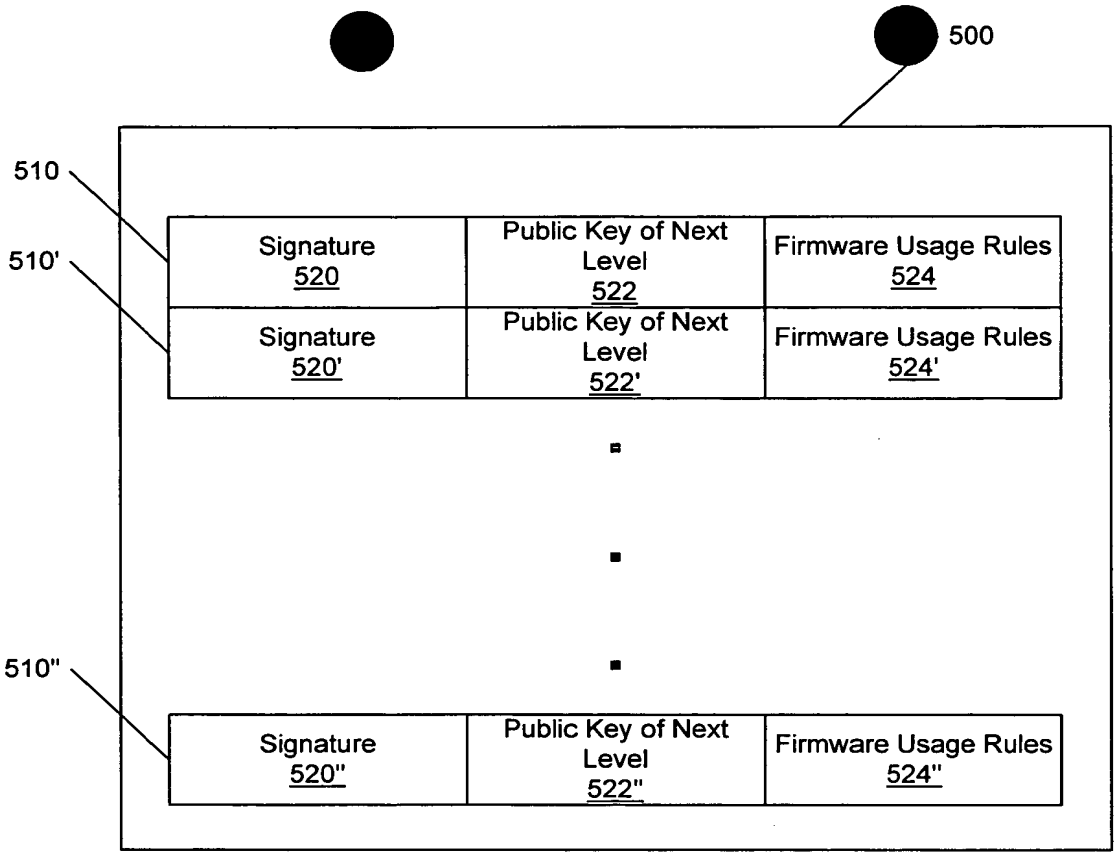

500
510
510'
510"
Signature
520
Public Key of Next Level
522
Firmware Usage Rules
524
Signature
520'
Public Key of Next Level
522'
Firmware Usage Rules
524'
Signature
520"
Public Key of Next Level
522"
Firmware Usage Rules
524"

Figure 7

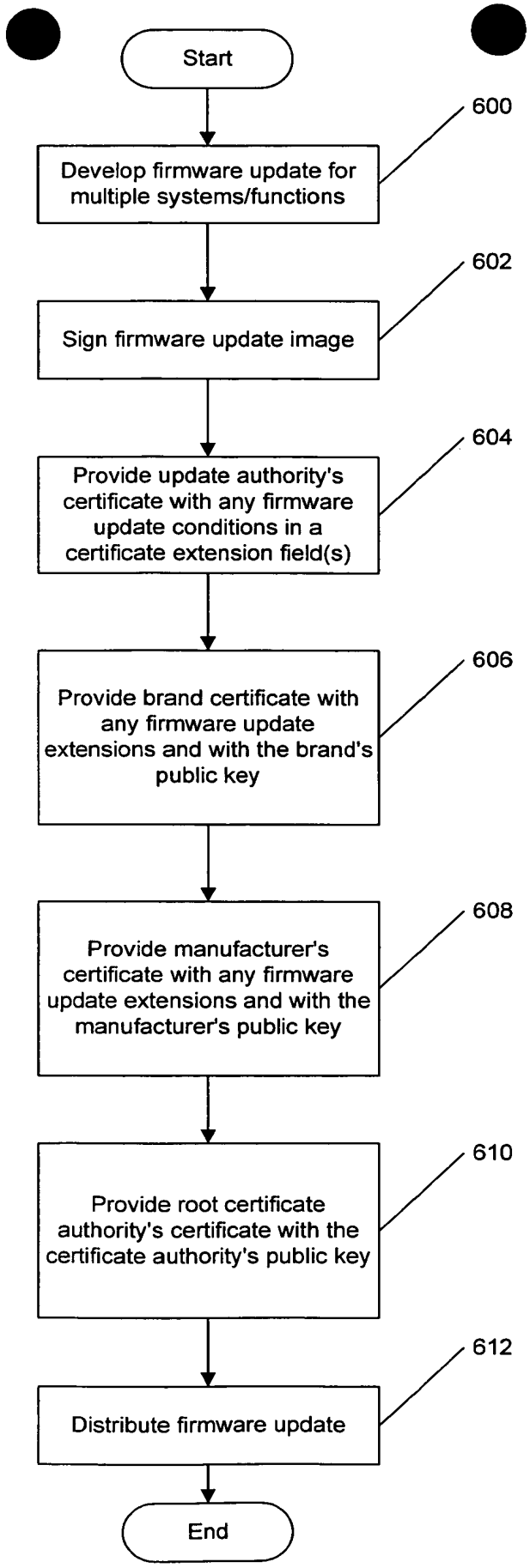

Start
600
Develop firmware update for multiple systems/functions
602
Sign firmware update image
604
Provide update authority's certificate with any firmware update conditions in a certificate extension field(s)
606
Provide brand certificate with any firmware update extensions and with the brand's public key
608
Provide manufacturer's certificate with any firmware update extensions and with the manufacturer's public key
610
Provide root certificate authority's certificate with the certificate authority's public key
612
Distribute firmware update
End

Figure 8

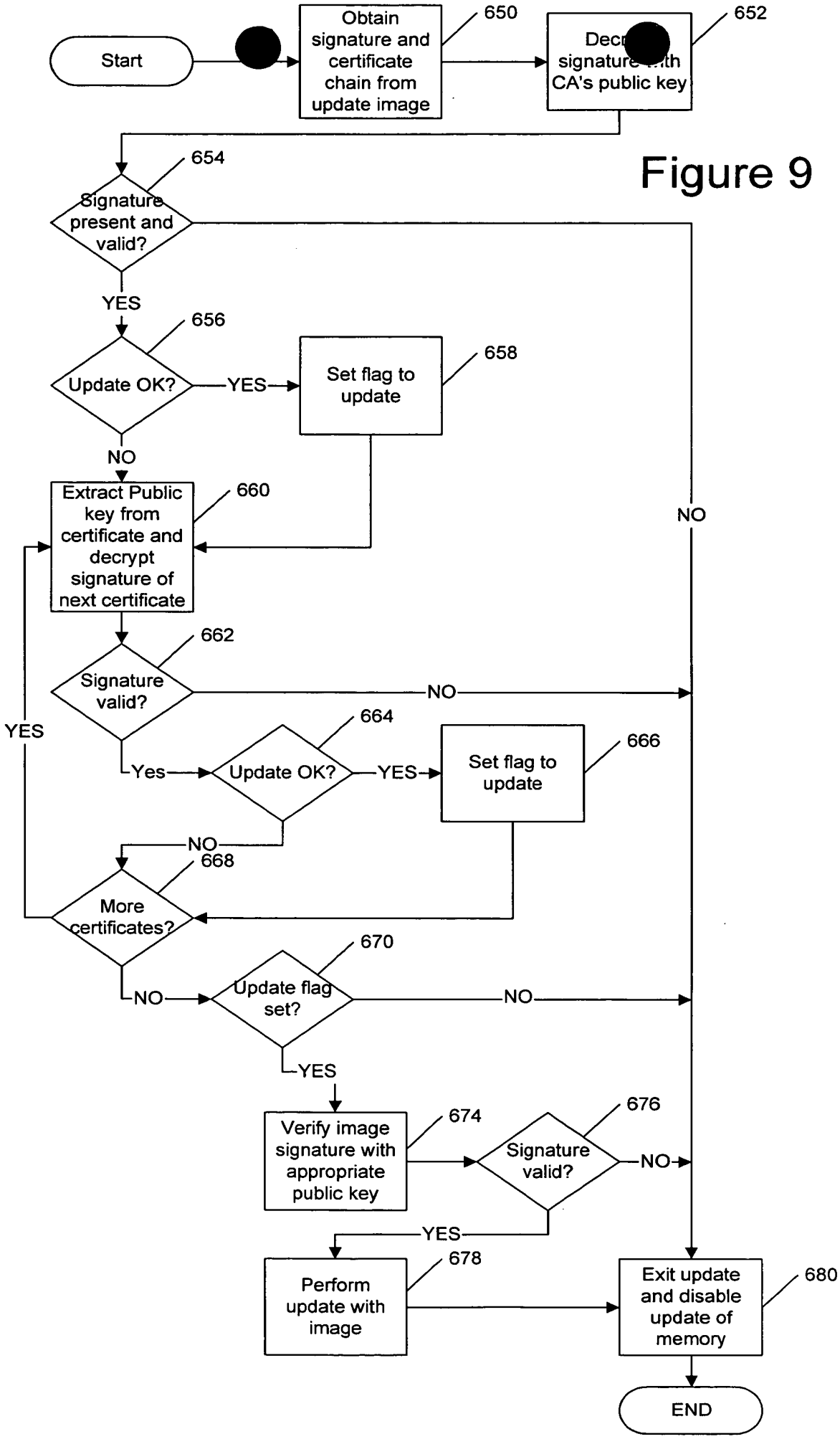

Start
Obtain signature and certificate chain from update image
650
Decr signature with CA's public key
652
654
Signature present and valid?
YES
NO
656
Update OK?
YES
Set flag to update
658
NO
Extract Public key from certificate and decrypt signature of next certificate
660
662
Signature valid?
NO
YES
664
Update OK?
YES
Set flag to update
666
NO
668
More certificates?
NO
670
Update flag set?
NO
YES
Verify image signature with appropriate public key
674
676
Signature valid?
NO
YES
678
Perform update with image
Exit update and disable update of memory
680
END

Figure 9

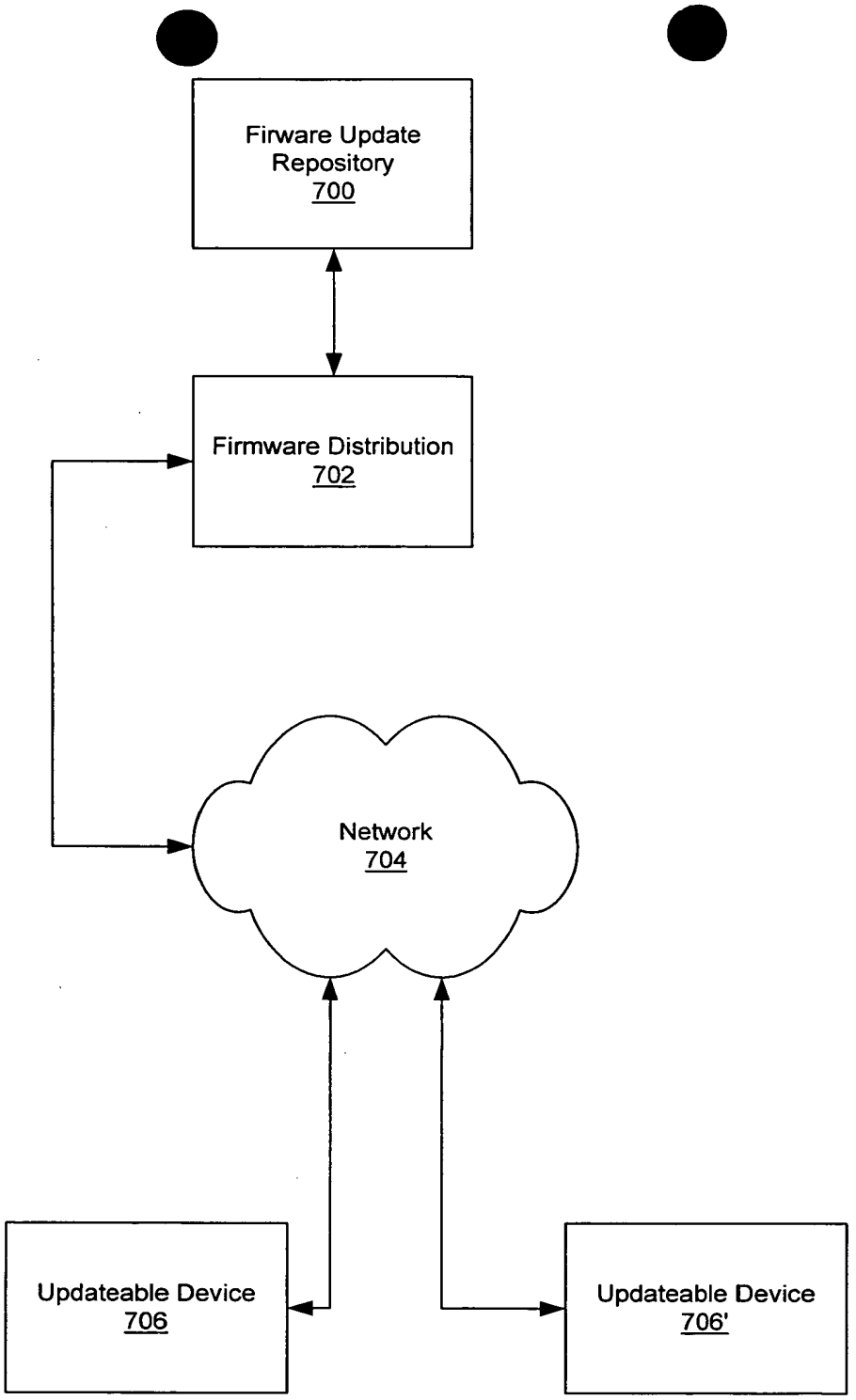

Firware Update Repository
700
Firmware Distribution
702
Network
704
Updateable Device
706
Updateable Device
706'

Figure 10

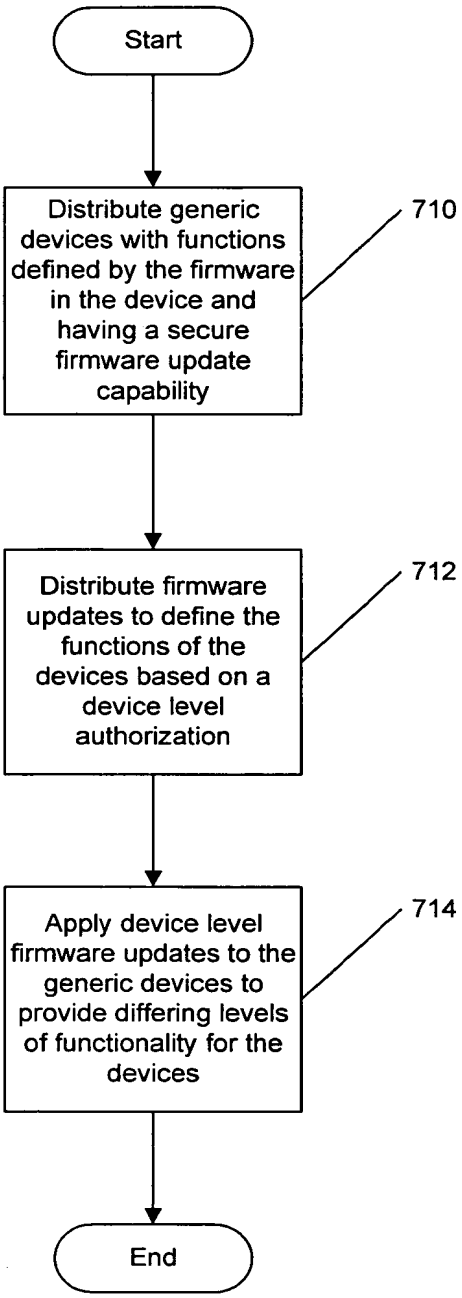

Start
Distribute generic devices with functions defined by the firmware in the device and having a secure firmware update capability
710
Distribute firmware updates to define the functions of the devices based on a device level authorization
712
Apply device level firmware updates to the generic devices to provide differing levels of functionality for the devices
714
End

Figure 11